REMARKS

The present application was filed on March 16, 2004 with claims 1-31. Claims 2-4, 17-19 and 31 were previously canceled. Claims 1, 5-16 and 20-30 remain pending, and claims 1 and 16 are the pending independent claims.

Claims 1, 5, 6, 9, 11, 12, 16, 20, 21, 24, 26 and 27 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2002/0161763 (hereinafter "Ye") in view of U.S. Patent Application Publication No. 2002/0107858 (hereinafter "Lundahl") and U.S. Patent No. 7,227,985 (hereinafter "Ikeda").

Claims 7, 10, 22, and 25 under 35 U.S.C. §103(a) as being unpatentable over Ye, Lundahl and Ikeda in view of U.S. Patent No. 6,625,585 (hereinafter "MacCuish").

Claims 8, 13-15, 23, and 28-30 are rejected under 35 U.S.C. §103(a) as being unpatentable over Ye, Lundahl and Ikeda in view of U.S. Patent Application Publication No. 2004/0098617 (hereinafter "Sekar").

As a preliminary matter, Applicants note that the Examiner has formulated rejections of dependent claims 11 and 26 over Ye, Lundahl and Ikeda in the present Office Action at page 8, second paragraph, and page 12, third paragraph, respectively. However, these claims appear to have omitted from the listing of claims rejected over Ye, Lundahl and Ikeda found in the present Office Action at page 3, first paragraph, which instead lists only claims 1, 5, 6, 9, 12, 16, 20, 21, 24 and 27 as having been so rejected. Accordingly, Applicants respectfully request that, in the event that an Advisory Action is issued responsive to the present submission, the Advisory Action should include a corrected indication of the grounds of rejection applicable to claims 11 and 26.

Claims 1 and 16 have been amended solely in order to correct a clear typographical error. Specifically, the phrase "at least no object" has been replaced with "no object." Support for this amendment may be found in the present specification at, for example, page 10, lines 15-20, and page 10, line 26, to page 11, line 2. The present amendment is believed to place the application in better form for consideration on appeal and is not believed to require further consideration or search; accordingly, entry under 37 CFR 1.116(b)(2) is respectfully requested.

Claims 1 and 16 include limitations wherein creating one or more clusters comprises, responsive to a determination that the similarity value is not greater than the threshold, determining whether there is at least one cluster to which no object has been added within a given period of time. Responsive to a determination that there is no cluster to which no object has been added within the given period of time, the object is added to the closest cluster and the statistical data of the closest cluster is updated. Responsive to a determination that there is at least one cluster to which no object has been added within the given period of time, the cluster to which no object has been added within the longest period of time is replaced with a new cluster comprising the object and statistical data of the new cluster is generated.

As described in the present specification at page 8, lines 10-26, with reference to an illustrative embodiment of the present invention:

> A newly created cluster containing only a single data point may be referred to as a "trend-setter." From the point of view of a user, a trend-setter is an outlier, until the arrival of other data points certify the fact that it is actually a cluster. If and when a sufficient number of new data points are added to the cluster, it is referred to as a mature cluster. The specific number of data points needed in order to make a mature cluster is application dependent, however, in the intrusion detection application described above, a mature cluster may contain 20-50 data points.
>
> At a given moment in time, a mature cluster can either be "active" or "inactive." A mature cluster is said to be active when it has received data points in the recent past. When a mature cluster has not received data points in the recent past, it is said to be inactive. Again, the specific amount of time that must pass in order for a mature cluster to become inactive is application dependent. However, in the intrusion detection application, an active mature cluster may be a mature cluster that has received data points in the last ten days. In some cases, a trend-setter cluster becomes inactive before it has a chance to mature. Such a cluster typically contains a small number of transient data points, which may typically be the result of an underlying abnormality that is short-term in nature.

As further described in the present specification at page 10, line 15, to page 11, line 4, again with reference to an illustrative embodiment of the present invention:

> In the case of cluster droplets described above, which maintain a maximum number of droplets k, the cluster with the maximum similarity value is defined as C_{mindex} If a similarity value of $S(X, C_{mindex})$ is greater than the user-defined threshold, the point X is assigned to the cluster C_{mindex}. It is also determined whether an inactive

cluster exists in the existing set of cluster droplets. If no such inactive cluster exists, then the data point X is added to C_{mindex}. In the even that the data point X is assigned to the cluster C_{mindex}, two steps are performed:

the statistics are updated to reflect the decay of the data points at the current moment in time; and

the statistics for each newly arriving data point are added to the statistics of C_{mindex}.

In the event that the newly arriving data point does not naturally fit in any of the cluster droplets and an inactive cluster does exist, then the most inactive cluster is replaced by a new cluster containing the solitary data point X. The most inactive cluster may be defined as the least recently updated cluster droplet. This new cluster is a potential outlier, or the beginning of a new trend. Further understanding of this new cluster droplet may only be obtained with the progress of the data stream.

In formulating the present rejections of claims 1 and 16, the Examiner relies on Ye, and more particularly paragraphs 41 and 42 thereof, as disclosing the limitations discussed above directed to determining whether there is at least one cluster to which no object has been added within a given period of time and then performing additional steps depending on the result of said determination. Applicants respectfully submit that the relied-upon portions of Ye contain no such teaching or suggestion. The remaining references of record fail to supplement this deficiency of Ye and hence the references of record fail to teach or suggest every limitation of independent claims 1 and 16.

Dependent claims 5-15 and 20-30 are patentable at least by virtue of their dependency from claims 1 and 16. Furthermore, these claims are believed to define separately patentable subject matter.

In view of the above, Applicants believe that claims 1, 5-16 and 20-30 are in condition for allowance, and respectfully request withdrawal of the §103(a) rejections.

Respectfully submitted,

/des/

Date: December 8, 2008

David E. Shifren
Attorney for Applicant(s)
Reg. No. 59,329
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2641